Dell EMC PowerStore

Configuring NFS Exports

2.x

June 2021
Rev. A01

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Preface

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this document are not supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features. Contact your service provider if a product does not function properly or does not function as described in this document.

Where to get help

Support, product, and licensing information can be obtained as follows:

- **Product information**

  For product and feature documentation or release notes, go to the PowerStore Documentation page at https://www.dell.com/powerstoredocs.

- **Troubleshooting**

  For information about products, software updates, licensing, and service, go to https://www.dell.com/support and locate the appropriate product support page.

- **Technical support**

  For technical support and service requests, go to https://www.dell.com/support and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

1

Overview

This chapter includes the following information.

Topics:

NFS support

PowerStore T model supports NFSv3 and NFSv4. It also supports secure NFS with Kerberos, for strong authentication. While PowerStore T model supports most of the NFSv4 and v4.1 functionality described in the relevant RFCs, directory delegation and pNFS are not supported. NFS support is enabled on a NAS server during or after creation, enabling you to create NFS-enabled file systems on that NAS server.

About secure NFS

You can configure secure NFS when you create or modify a NAS server that supports UNIX shares. Secure NFS provides Kerberos-based user authentication, which can provide network data integrity and network data privacy.

Kerberos is a distributed authentication service designed to provide strong authentication with secret-key cryptography. It works on the basis of "tickets" that allow nodes communicating over a non-secure network to prove their identity in a secure manner. When configured to act as a secure NFS server, the NAS server uses the RPCSEC_GSS security framework and Kerberos authentication protocol to verify users and services.

Security options

Secure NFS supports the following security options:

- krb5: Kerberos authentication
- krb5i: Kerberos authentication and data integrity by adding a signature to each NFS packet transmitted over the network
- krb5p: Kerberos authentication, data integrity, and data privacy by encrypting the data before sending it over the network

  Data encryption requires more resources for system processing and can lead to slower performance.

In a secure NFS environment, user access to NFS file systems is granted based on Kerberos principal names. However, access control to shares within a file system is based on the UNIX UID and GID, or on ACLs.

NOTE: Secure NFS supports NFS credentials with more than 16 groups, which is equivalent to the extended UNIX credentials option.

Configuring secure NFS

If you are implementing Secure NFS, configure the following:

- At least one NTP server must be configured on the PowerStore appliance to synchronize the date and time. It is recommended that you set up a minimum of two NTP servers per domain to avoid a single point of failure.
- A UNIX Directory Service (UDS)
- One or more DNS servers
- Either an AD or custom realm must be added for Kerberos authentication
- A keytab file must be uploaded to your NAS server when using a custom realm in a Kerberos configuration

Planning considerations

Review the following information before configuring NFS exports:

File storage support is only available with PowerStore T model appliances. File storage is not supported with PowerStore X model appliances.

NAS server networks

Creating network VLANs and IP addresses is optional for NAS servers. If you plan to create a VLAN for NAS servers, the VLAN cannot be shared with the PowerStore T model management, or storage networks. Also, be sure to work with your network administrator to reserve the network resources and configure the network on the switch. See the *PowerStore Networking Guide for PowerStore T Models* for details.

Deployment requirements

NAS services are only available on PowerStore T model appliances. If you are running PowerStore X model appliances, this service is not available.

You must have chosen **Unified** during initial configuration of your PowerStore T model appliance. If you chose **Block Optimized** while running the Initial Configuration Wizard, NAS services were not installed. To install NAS services, you will need to have your system reinitialized by a customer support representative. Reinitializing the system:

- Sets the appliance back to the factory state.
- Removes all configuration that was done on the system through the **Initial Configuration Wizard**.
- Removes any configuration that is performed in PowerStore after initial configuration.

More considerations

Both nodes on the appliance must be up and running to create a NAS server. If one of the nodes is down on the appliance, NAS server creation will fail.

Creating NFS exports

Complete the following before you can create NFS exports in PowerStore:

1. Create NAS servers with NFS protocol
2. Create a file system for NFS exports

Documentation resources

Refer to the following for additional information:

Table 1. Documentation resources

Document	Description	Location
PowerStore Networking Guide for PowerStore T Models	Provides network planning and configuration information.	https://www.dell.com/powerstoredocs
PowerStore Configuring SMB Shares Guide	Provides information necessary to configure SMB shares with PowerStore Manager.	
Dell EMC PowerStore File Capabilities White Paper	Discusses the features, functionality, and protocols supported by Dell EMC PowerStore file architecture.	
PowerStore Online Help	Provides context-sensitive information for the page opened in PowerStore Manager.	Embedded in PowerStore Manager

2

Create NAS servers

This chapter includes the following information.

Topics:

Overview of configuring NAS servers

Before you can provision file storage on the storage system, a NAS server must be running on the system. A NAS server is a file server that uses the SMB protocol, NFS protocol, or both to share data with network hosts. It also catalogs, organizes, and optimizes read and write operations to the associated file systems.

This document describes how to configure a NAS server with NFS protocol, on which file systems with NFS exports can be created.

Create a NAS server for NFS (UNIX-only) file systems

You create NAS servers before creating file systems.

Be sure to have your NAS network information available.

1. Select **Storage** > **NAS Servers**.
2. Select **Create**.
3. Continue to work through the **Create NAS Server** wizard.

Wizard Screen	Description
Details	Enter a NAS Server name, description, and network information. **NOTE:** You cannot reuse VLANs that are being used for the management and storage networks.
Sharing Protocol	**Select Sharing Protocol** Select NFSv3, or NFSv4, or both. **NOTE:** If you select SMB and an NFS protocol, you automatically enable the NAS server to support multiprotocol. **Unix Directory Services** (Naming Services) You can configure the naming services with a combination of Local Files and NIS, or LDAP. Refer to the following sections for configuring: ● Using Local Files ● With NIS ● With LDAP You can choose to enable Secure NFS here. Secure NFS requires the following:

Wizard Screen	Description
	• At least one NTP server must be configured on the PowerStore appliance to synchronize the date and time. It is recommended that you set up a minimum of two NTP servers per domain to avoid a single point of failure. • A UNIX Directory Service (UDS) • One or more DNS servers • Either an AD or custom realm must be added for Kerberos authentication • A keytab file must be uploaded to your NAS server when using a custom realm in a Kerberos configuration **DNS** DNS server information is mandatory when: • Joining an AD domain, but optional for a stand-alone NAS server. • Configuring Secure NFS. DNS can also be used to resolve hosts defined on NFS export access lists.
Summary	Review the content and Select **Previous** to go back and make any corrections.

4. Select **Create NAS Server** to create the NAS server.
   The **Status** window opens, and you are redirected to the **NAS Servers** page once the server is listed on the page.

Once you have created the NAS server for NFS, you can continue to configure the server settings.

If you enabled Secure NFS, you must continue to configure Kerberos.

Select the NAS server to continue to configure, or edit the NAS server settings.

Configure NAS Server Naming Services

You can configure, or modify the naming services for a NAS Server.

Naming Services include configuring one or more of the following:

- DNS
- NIS for Unix Directory Services (UDS)
- LDAP for UDS
- Local Files

Configure DNS

You can disable DNS, or enable and configure a NAS server to use DNS.

DNS can also be used to resolve hosts defined on NFS export access lists.

DNS is required for:

- Secure NFS
- Joining an AD domain.

You cannot disable DNS for NAS servers that are configured with:

- Multiprotocol file sharing
- SMB file sharing that is joined to an Active Directory (AD)
- Secure NFS

1. Select **Storage** > **NAS Servers** > **[nas server]** > **DNS**.
2. Enable or disable DNS. If you enabled DNS, enter the DNS server information.

Configure the NAS server UNIX Directory Service for NIS

You can configure NAS server UNIX Directory Service (UDS) for NIS.

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS** card.
2. If **Disabled** is on, slide the button to change to **Enabled**.
3. In the **Unix Directory Service** drop down, select **NIS**.
4. Enter an NIS **Domain** and add the IP **Addresses** for the NIS servers.
5. Select **Apply**.

To troubleshoot issues with configuring a UDS using NIS, ensure that the NIS server domain and server IP addresses you enter are correct.

Configure a NAS server UNIX Directory Service using LDAP

You can configure a NAS server UNIX Directory Service (UDS) using LDAP.

LDAP must adhere to the IDMU, RFC2307, or RFC2307bis schemas. Some examples include AD LDAP with IDMU, iPlanet, and OpenLDAP. The LDAP server must be configured properly to provide UIDs for each user. For example, on IDMU, the administrator must go in to the properties of each user and add a UID to the UNIX Attributes tab.

You can configure LDAP to use anonymous, simple, and Kerberos authentication. If using Kerberos authentication, you must configure the following before you continue to configure LDAP with Kerberos:

1. From the **Naming Services** card, configure the DNS server that is used to join and unjoin a Kerberos server to a realm.
2. From the **Security** card, add the Kerberos Realm.
1. Select **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS** card.
2. If **Disabled** is on, slide the button to change to **Enabled**.
3. In the **Unix Directory Service** drop down, select **LDAP**.
4. Leave the default or enter a different **Port Number**.

   NOTE: By default, LDAP uses port 389, and LDAP over SSL (LDAPS) uses port 636.

5. Add the IP addresses for the LDAP servers.

   The NAS server can be configured to use the DNS service discovery to automatically obtain LDAP server IP addresses.

   NOTE: For this discovery process to work, the DNS server must contain pointers to the LDAP servers, and the LDAP servers must share the same authentication settings.

6. Configure the LDAP authentication as described in the following table:

Option	Description
Anonymous	Specify the Base DN, and the Profile DN for the iPlanet/OpenLDAP server.

Simple	Specify the following:
	• If using AD, LDAP/IDMU:
	  ○ Bind DN in LDAP notation format; for example, **`cn=administrator,cn=users,dc=svt,dc=lab,dc=com`**.
	  ○ Base DN, which is the same as the Fully Qualified Domain Name (for example, **`svt.lab.com`**).
	  ○ Profile DN.
	• If using the iPlanet/OpenLDAP server:
	  ○ Bind DN in LDAP notation format; for example, **`cn=administrator,cn=users,dc=svt,dc=lab,dc=com`**.
	  ○ Password
	  ○ Base DN. For example, if using **`svt.lab.com`**, the Base DN would be **`DC=svt,DC=lab,DC=com`**.
	  ○ Profile DN for the iPlanet/OpenLDAP server.

Kerberos	Configure a custom realm to hover over any type of Kerberos realm (Windows, MIT, Heimdal). With this option, the NAS Server uses the custom Kerberos realm that is defined in the Kerberos subsection of the NAS server **Security** tab.

Option	Description
	NOTE: If you use NFS secure with a custom realm, you have to upload a keytab file.

7. Select **Retrieve Current Schema** to download the ldap.conf file.
8. Edit and save the `ldap.conf` file.
9. Select **Upload New Schema** to upload the updated `ldap.conf` file.
10. Optionally, enable LDAP Secure (Use SSL), and upload the CA certificate.

To troubleshoot issues with configuring a UDS using LDAP, ensure that:

- The LDAP configuration adheres to one of the supported schemas, as described earlier in this topic.
- The containers that are specified in the `ldap.conf` file hover over containers that are valid and exist.
- Each LDAP user is configured with a unique UID.

Configure NAS server to use local files for naming services

You can configure your naming services to use local files.

- Local files can be used instead of, or also with DNS, LDAP, and NIS directory services.
- If you configure local files with a UNIX Directory Service (UDS), the storage system queries the local files first.
- After you finish creating the NFS server, you can go back and upload more local files.
- Once the NAS server is created, enable the local files as described in the following steps:

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **Local Files**.
2. For each type of local file, select the down arrow to download the current file. If there is no file on the storage system, the system downloads a file template.
3. Update the file with your system information.

   To use local files for FTP access, the `passwd` file must include an encrypted password for the users. This password is used for FTP access only. The `passwd` file uses the same format and syntax as a standard UNIX system, so you can apply the password to generate the local `passwd` file. On a UNIX system, use `useradd` to add a user and `passwd` to set the password for that user. Then, copy the hashed password from the `/etc/shadow` file, add it to the second field in the `/etc/passwd` file, and upload the `/etc/passwd` file to the NAS server.
4. Save the updated file to your local machine.
5. Select **Upload Local Files** and browse to the location of the file you edited and select the file to upload.
6. Repeat for each type of file.

To troubleshoot issues with configuring local files, ensure that:

- The file is created with the proper syntax. (Six colons are required for each line.) Reference the template for more details about the syntax and examples.
- Each user has a unique name and UID.

Configure NAS server Sharing Protocols

You can configure or modify the sharing protocols that are configured for a NAS server.

Configuring sharing protocols for NFS includes setting up one or more of the following:

- NFS Server
- FTP

Configure NFS Server

Configure the NAS server for UNIX-only systems, or modify the NFS server settings.

DNS and NTP must be configured before configuring a Secure NFS server.

1. Select the **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **NFS Server** tab.
2. Enable the **Linix/UNIX shares** option to define the NAS server for UNIX support.

3. Enable either **NFSv3**, **NFSv4**, or both.
4. Optionally, disable, or enable Secure NFS.
   Extended UNIX credentials are also enabled.
5. **Enable or disable Extend Unix** credentials.

   NOTE: Secure NFS supports NFS credentials with more than 16 groups, which is equivalent to the extended UNIX credentials option.

   - If this field is selected, the NAS server uses the User ID (UID) to obtain the primary Group ID (GID) and all group GIDs to which it belongs. The NAS server obtains the GIDs from the local password file or UDS.
   - If this field is cleared, the UNIX credential of the NFS request is directly unzipped from the network information that is contained in the frame. This method has better performance, but it is limited to including up to only 16 group GIDs.
6. In the **Credential Cache Retention**, enter a time period (in minutes) for which access credentials are retained in the cache.
7. **Apply** the changes.

Configure FTP, or SFTP sharing protocol

You can configure FTP or FTP over SSH (SFTP) settings for an existing NAS server only.

Passive mode FTP is not supported.

FTP access can be authenticated using the same methods as NFS. Once authentication is complete, access is the same as NFS for security and permission purposes. If the format is anything other than `user@domain` or `domain\user`, NFS authentication is used. NFS authentication uses local files, LDAP, NIS, or local files with LDAP or NIS.

To use local files for NFS, FTP access, the `passwd` file must include an encrypted password for the users. This password is used for FTP access only. The `passwd` file uses the same format and syntax as a standard Unix system, so you can leverage this to generate the local `passwd` file. On a Unix system, use `useradd` to add a new user and `passwd` to set the password for that user. Then, copy the hashed password from the `/etc/shadow` file, add it to the second field in the `/etc/passwd` file, and upload the `/etc/passwd` file to the NAS server.

1. Select the **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **FTP** tab.
2. Under **FTP**, if Disabled in on, slide the button to **Enable**.
3. Optionally also enable SSH FTP. Under **SFTP**, if Disabled in on, slide the button to **Enable**.
4. **Under FTP/SFTP Server Access**, Select which type of authenticated users have access to the files.
5. Optionally, show the **Home Directory and Audit** options.
   - Select or clear the **Home directory restrictions**. If disabled, enter the **Default home directory**.
   - Select or clear **Enable FTP/SFTP Auditing**. If checked, enter the directory location of where to save the audit files, and the maximum size allowed for the audit file.
6. Optionally, **Show Messages**, and enter a default **Welcome message**, and **Message of the day**.
7. Optionally, **Show Access Control List** to provide access or deny access to **Filtered Users**, **Filtered Groups**, and **Filtered hosts**.
8. Click **Apply**.

Configure Kerberos for NAS server Security

You can configure the NAS Server with Kerberos.

Kerberos is a distributed authentication service designed to provide strong authentication with secret-key cryptography. It works on the basis of "tickets" that allow nodes communicating over a non-secure network to prove their identity in a secure manner. When configured to act as a secure NFS server, the NAS server uses the RPCSEC_GSS security framework and Kerberos authentication protocol to verify users and services.

If the NAS server has been configured with NFS only, and you are configuring Secure NFS, or LDAP with Kerberos, you must configure Kerberos with a custom realm before configuring security in PowerStore.

If the NAS server has been configured with both the NFS and SMB protocol, you have the option of using Kerberos that is inherited with AD since the domain joined SMB server exists on the NAS server.

The storage system must be configured with an NTP server. Kerberos relies on the correct time synchronization between the KDC, servers, and client on the network.

Configuring Kerberos for Secure NFS

If you are configuring Kerberos for Secure NFS, be aware of the following:

- If configuring the NAS server for NFS only, you must configure the NAS server with a custom realm. If you have configured the NAS server with NFS and SMB, you can use either the AD or custom realm.
- Using LDAPS or LDAP with Kerberos is recommended for increased security.
- A DNS server must be configured at the NAS-server level. All members of the Kerberos realm, including the KDC, NFS server, and NFS clients, must be registered in the DNS server.
- The NFS client's hostname FQDN and NAS server FQDN must be registered in the DNS server. Clients and servers must be able to resolve any member of the Kerberos realm's FQDNs to an IP address.
- The FQDN part of the NFS client's SPN must be registered in the DNS server.
- A keytab file must be uploaded to your NAS server when configuring Secure NFS.

Create a custom realm for Kerberos

You can configure a custom realm to use with Kerberos.

A custom Kerberos realm lets you configure any kind of KDC (MIT/Heidmal or AD). Use this method when you do not have an SMB server domain that is configured on the NAS server or if you want to use a different Kerberos realm than the one configured for the SMB server.

Create custom realm for pure NFS Server

To use a Unix-based KDC, follow these steps before configuring Kerberos in PowerStore. The steps assume that you want to use myrealm in the Kerberos realm linux.dellemc.com as the hostname of the NFS server.

1. Run the `kadmin.local` tool.
2. Create the principals and their keys:

   ```
   kadmin.local: addprinc -randkey nfs/myrealm.linux.dellemc.com
   ```

   and/or

   ```
   kadmin.local: addprinc -randkey nfs/myrealm
   ```

3. Put the key of the principal into the keytab file myrealm.linux.dellemc.fr:

   ```
   kadmin.local: ktadd -k myrealm.linux.dellemc.com.keytab nfs/myrealm.linux.dellemc.fr
   ```

Create custom realm for multiprotocol (NFS and SMB) NAS server

To use a Windows-based KDC without using the SMB server account on the NAS server, follow these steps before configuring Kerberos in PowerStore. The steps assume that you want to use myrealm.windows.dellemc.com as the FQDN for the NFS server.

1. Create account myrealm for the NAS server in the Active Directory (AD) of the windows domain windows.dellemc.com.
2. Register the service SPN on the computer account you created:

   ```
   C:\setspn -S nfs/myrealm.windows.dellemc.com myrealm
   ```

3. Verify that the SPN was created.

   ```
   C:\setspn myrealm
   ```

4. Generate a keytab file for the SPN:

   ```
   C:\ktpass -princ nfs/myrealm.windows.dellemc.com@WINDOWS.DELLEMC.COM -mapuser
   WINDOWS\myrealm
    -crypto ALL +rndpass -ptype KRB5_NT_PRINCIPAL -out myrealm.windows.dellemc.com.keytab
   ```

Configure Kerberos security for the NAS server

You can configure the NAS server with Kerberos security.

If configuring for NFS, DNS and UDS must be configured for the NAS server and all members of the Kerberos realm must be registered in the DNS server.

If using a NAS server that is configured for both SMB and NFS, be sure to add the SMB server to the AD domain.

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Security** > **Kerberos**.
2. If Disabled is on, slide the button to change to **Enabled**.
3. Enter the name of the **Realm**.
4. Enter the **Kerberos IP Address** and click **Add**.
5. Enter the TCP Port for Kerberos to use. 88 is the default port.
6. Click **Apply**.

If you choose to change from an AD realm to a custom realm after the NAS server is successfully created with Secure NFS, you cannot mount any NFS exports until you perform the following operations:

1. Create a Keytab file.
2. Remove the AD realm from the NAS server.
3. Enter the Username and Password for the AD Server.
4. Enter the custom realm.
5. Upload the Keytab file.

3

Configure NFS Exports

This chapter includes the following information:

Topics:

File systems and NFS Exports overview

While creating File Systems and NFS Exports, it is helpful to note the following:

- A NAS server must be configured to support NFS protocol before creating a file system.
- You can choose to add NFS Exports the first time you create the file system, or you can add NFS Exports to a file system after it has been created.

Create a file system for NFS exports

You can create a file system for NFS exports.

Make sure that there is a NAS server that is configured to support the NFS protocol.

1. Select **Storage** > **File Systems**.
2. Click **Add**.
   The **Add File System** wizard launches.
3. Select an NFS enabled NAS server for the file system.
4. Specify the file system details, including the file system name and size, minimum size is 3 GB, maximum size is 256 TB.

   NOTE: All thin file systems, regardless of size, have 1.5GB reserved for metadata upon creation. For example, after creating a 100GB thin file system, PowerStore T model immediately shows 1.5GB used. When the file system is mounted to a host, it shows 98.5GB of usable capacity.

   This is because the metadata space is reserved from the usable file system capacity.

5. Configure the initial export for the file system.

   NOTE: You can add NFS exports to the file system at later time.

6. Configure Host Access.

Option	Description
Minimum Security	Select **Sys** to allow users with non-secure NFS, or Secure NFS to mount and NFS export on the file system. If you are not configuring Secure NFS you must select this option. If you are creating a file system with Secure NFS, then you can choose from the following options: • **Kerberos** to allow any type of Kerberos security for authentication (krb5/krb5i/krb5p). • **Kerberos with Integrity** to allow both Kerberos with integrity and Kerberos with encryption security for user authentication (krb5i/krb5p). • **Kerberos with Encryption** to allow only Kerberos with encryption security for user authentication (krb5p).
Default Access	The type of access that is applied to the hosts by default. Optionally, you can choose a different type of access to the host when adding individual hosts. Options include:

Option	Description
	• **No Access** — No access permitted to the storage resource or share. • **Read/Write** — Hosts have permission to view the contents of the storage resource or share, but not to write to it. • **Read-Only** — Hosts have permission to read and write to the NFS datastore or share. **NOTE:** ESXI hosts must have **Read//Write** access in order to mount an NFS datastore using NFSv4 with **Kerberos NFS owner** authentication. • **Read/Write, allow Root** — Hosts have permission to read and write to the storage resource or share, and to grant revoke access permissions (for example, permission to read, modify and execute specific files and directories) for other login accounts that access the storage. The root of the NFS client has root access to the share. **NOTE:** Unless the hosts are part of a supported cluster configuration, a void granting Read/Write access to more than one host. **NOTE:** ESXi hosts must have **Read/Write, allow Root** access in order to mount an NFS datastore using NFSv4 with NFS Owner:root authentication. • **Read-Only, allow Root** — Hosts have permission to view the contents of the share, but not to write to it. The root of the NFS client has root access to the share.
Add Host	Enter hosts individually, or you can add hosts by uploading a properly formatted CSV file. You can download the CSV file first to obtain a template. To download, edit, and use a CSV file template: a. Click the **Export Hosts** icon. b. Update the CSV file with the hosts, and access types you want to import. c. Save the CSV file to your local machine. d. Click **Import CSV file**. e. Browse to the CSV file, and click **Open** in your Microsoft File Explorer window. The hosts from the CSV file appear in the **Import Host List** with the **Access Type** you defined in the CVS file.

Option	Description
Local path	The path to the file system storage resource on the storage system. This path specifies the unique location of the share on the storage system. • Each NFS share must have a unique local path.PowerStore automatically assigns this path to the initial export created within a new file system. The local path name is based on the file system name. • Before you can create more exports within an NFS file system, create a directory to share from a Linux/ UNIX host that is connected to the file system. Then you can create an export from PowerStore and set access permissions accordingly.
Export path	The path used by the host to connect to the export. PowerStore creates the export path that is based on the IP address of the host, and the name of the export. Hosts use either the file name or the export path to mount or map to the export from a network host.

7. Optionally, add a protection policy to the file system.
   If you are adding a protection policy to the file system, the policy must have been created before creating the file system. Only snapshots are supported for protection for file systems. Replication is not supported on file system.
8. Review the summary and click **Create File System**.
   The file system is added to the **File System** tab. If you created an export simultaneously, then the export displays in the **NFS export** tab.

Create an NFS export

You can create an NFS export on a file system.

1. Select the **Storage** > **File Systems** > **NFS Export** tab.
2. Click **Create**.
   The **Create NFS Export** wizard launches.
3. Enter the requested information while noting the following:
   - Snapshots must have been created before creating the NFS export.

- **Local Path** must correspond to an existing folder name within the file system that was created from the host-side.
- The value specified in the **NFS Export Details**, **Name** field, along with the NAS server name, constitutes the name by which hosts access the export.
- NFS export names must be unique at the NAS server level per protocol. However, you can specify the same name for an SMB share, and NFS exports.

4. Once you approve the settings, click **Create NFS Export**.
   The NFS Export displays on the **NFS Export** page.

4

Additional NAS Server Features

This chapter includes the following.

Topics:

Set the preferred UNIX Directory Service

After you have created a NAS server, you can set the preferred UNIX Directory Services (UDS) search order for user access.

1. Select **Storage** > **NAS Servers**.
2. Select the checkbox in the **Name** column to the left of the NAS server.
3. Click **Modify**.
4. Select the preferred UDS search order for use from the list of **Unix Directory Service Search Order** drop down.
5. Click **Apply**.

Configure NAS server networks

You can modify or configure NAS server networks.

Configure the following for NAS server networks:

- The file interfaces
- Routes to external services such as hosts.

Configure file interfaces for a NAS Server

You can configure the file interfaces for a NAS server after the server has been added to PowerStore.

You can add more file interfaces, and define which is the preferred interface to use. Also, you can define which interface to use for production and backup, or for IPv4, or IPv6.

1. Select **Storage** > **NAS Servers** > **[nas server]**.
2. Click **Add** to add another file interface to the NAS server.
3. Enter the File Interface properties.

   NOTE: You cannot reuse VLANs that are being used for the management and storage networks.

4. You can perform the following on a File Interface by selecting a file interface from the list. Click:

Option	Description
Modify	To change the properties of the file interface properties.
Delete	To delete the file interface from the NAS server.
Ping	To test the connectivity from the NAS server to the external IP address.
Preferred Interface	To define which interface PowerStore should default to using when multiple production and backup interfaces have been defined.

Configure routes for the file interface for external connections

You can configure the routes that the file system uses for external connections.

You can use the **Ping** option from the **File Interface** card to determine if the file interface has access to the external resource.

Usually, the NAS server interfaces are configured with a default gateway, which is used to route requests from the NAS server interface to external services.

Use the following steps:

- If you need to configure more granular routes to external services.
- To add a route to access a server from a specific interface through a specific gateway.

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Networks** > **Routes to External Services**.
2. Click **Add** to enter the route information in the **Add Route** wizard.

Enable NDMP Protection and Events

You can configure standard backup for the NAS servers using NDMP. The Network Data Management Protocol (NDMP) provides a standard for backing up file servers on a network. Once NDMP is enabled, a third-party Data Management Application (DMA), such as Dell EMC Networker, can detect the PowerStore NDMP using the NAS server IP address.

Enabling NDMP is performed after the NAS server is created.

PowerStore supports:

- Three-way NDMP. The data is transferred through the DMA over a local area network (LAN) or Wide Area Network (WAN).
- Full and incremental backups.

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Protection and Events** .
2. Under **NDMP Backup**, if **Disabled** is on, slide the button to change to **Enabled**.
3. Enter a password for the **New Password**.
   The user name is always `ndmp`.
4. Re-enter the same password as the new password in **Verify Password**.
5. Click **Apply**.

Leave the NDMP page, and return back to the NDMP page to validate that NDMP is enabled.

5

More file system features

This chapter includes the following information.

Topics:

File system quotas

You can track and limit drive space consumption by configuring quotas for file systems at the file system or directory level. You can enable or disable quotas at any time, but it is recommended that you enable or disable them during non-peak production hours to avoid impacting file system operations.

NOTE: You cannot enable quotas for read-only file systems.

Types of quotas

There are three types of quotas you can put on a file system.

Table 2. Quota types

Type	Description
User Quotas	Limits the amount of storage that is consumed by an individual user storing data on the file system.
Tree Quota	Tree quotas limit the total amount of storage that is consumed on a specific directory tree. You can use tree quotas to: • Set storage limits on a project basis. For example, you can establish tree quotas for a project directory that has multiple users sharing and creating files in it. • Track directory usage by setting the tree quota hard and soft limits to 0 (zero). **NOTE:** If you change the limits for a tree quota, the changes take effect immediately without disrupting file system operations.
User quota on a quota tree	Limits the amount of storage that is consumed by an individual user storing data on the quota tree.

Quota Limits

Table 3. Hard and Soft Limits

Type	Descriptions
Hard	A hard limit is an absolute limit on storage usage. If a hard limit is reached for a user quota on a file system or quota tree, the user cannot write data to the file system or tree until more space becomes available. If a hard limit is reached for a quota tree, no user can write data to the tree until more space becomes available.
Soft limit	A soft limit is a preferred limit on storage usage. The user is allowed to use space until a grace period has been reached. The user is alerted when the soft limit is reached, until the grace period is over. After that, an out of space condition is reached until the user gets back under the soft limit.

Quota Grace Period

The Quota Grace Period, provides the ability to set a specific grace period to each tree quota on a file system. The grace period counts down the time between the soft and hard limit, and alerts the user about the time remaining before the hard limit is met. If the grace period expires you can not write to the file system until more space has been added, even if the hard limit has not been met.

You can set an expiration date for the Grace Period. The default is 7 days, alternatively you can set the Grace Period expiration date to an infinite amount of time and the Grace Period will never expire, or for specified number of days, hours or minutes. Once the Grace Period expiration date is met, the Grace Period will no longer apply to the File System directory.

Additional information

For more information on quotas, see the *Dell EMC PowerStore File Capabilities White Paper*.

Enable User Quotas

You must enable Quotas and set the User Quota defaults before you can add a User Quota to a files system.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas**.
2. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Properties**.
3. Slide the **Disabled** button to the right until it is **Enabled**.
4. Enter the default **Grace Period** for the user quota on the file system which will count down time after the soft limit is met until the hard limit will be met.
5. Enter a default **Soft Limit**, and a default **Hard Limit** and click **Update**.

Add a user quota onto a file system

Create a user quota on a file system to limit or track the amount of storage space that individual users consume on that file system. When you create or modify user quotas, you can use default hard and soft limits that are set at the file-system level.

You must enable Quotas and set the User Quota defaults before you can add a User Quota to a files system. See Enable User Quotas.

NOTE: You cannot create quotas for read-only file systems.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **User**.
2. Select **Add** on the **User Quota** page.
3. In the **Add User Quota** wizard, provide the requested information. To track space consumption without setting limits, set **Soft Limit** and **Hard Limit** to 0, which indicates no limit.
4. Select **Add**.

Add a quota tree onto a file system

Create a quota tree at the directory level of a file system to limit or track the total storage space that is consumed for that directory.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Select **Add**.
3. Slide the **Enforce User Quota** to the right to enabled User Quota defaults on the Tree Quota.
4. Provide the requested information.
   - Enter a **Grace Period** to count down the time between the soft and hard limit. You will begin to receive alerts once the grace period is reached.
   - To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.
5. Select **Add**.

Add a user quota onto a quota tree

Create a user quota on a quota tree to limit or track the amount of storage space that individual users consume on that tree. When you create user quotas on a tree, you can to use the default grace period and default hard and soft limits that are set at the tree-quota level.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Select a path, and click **Add User Quota**.
3. On the **Add User Quota** screen, provide the requested information. To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.